September 20, 2021

Re: Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program, Docket No. 21-232 & No. 21-233

IPVM is a research organization focused on surveillance businesses and technologies. Our work is cited by Congress and regularly featured in the national press,[1][2] and we have published hundreds of reports on Hikvision and Dahua over the past decade. The position we express here is the product of our detailed knowledge of the companies' global operations, personnel, products, and activities.

The evidence shows that Hikvision and Dahua are a danger to national security.

New Vulnerabilities

Just today, we reported on a new critical vulnerability in Hikvision products.[3] The researcher who discovered this declared it to be "the highest level of critical vulnerability - a zero click unauthenticated remote code execution".[4]

Only two weeks ago, we reported on two new critical vulnerabilities in Dahua products.[5]

Both Dahua and Hikvision's vulnerabilities would allow hackers to access camera feeds and recordings, switch devices on or off, reposition cameras, hack into the networks to which they are connected, or use the devices in a botnet attack. We estimate this impacts more than ten million devices in the United States, making surveillance networks at tens of thousands of sites across the US vulnerable; due to the widespread relabelling of

---

[1] Chinese Surveillance-Gear Maker Hikvision Has Ties to Country's Military, Report Says https://www.wsj.com/articles/chinese-surveillance-gear-maker-hikvision-has-ties-to-countrys-military-report-says-11621941983?mod=hp_lead_pos4

[2] Major camera company can sort people by race, alert police when it spots Uighurs https://www.latimes.com/business/technology/story/2021-02-09/dahua-facial-recognition-china-surveillance-uighur

[3] Hikvision Has "Highest Level of Critical Vulnerability", Impacting 100+ Million Devices https://ipvm.com/reports/hikvision-36260

[4] Unauthenticated Remote Code Execution (RCE) vulnerability in Hikvision IP camera/NVR firmware (CVE-2021-36260) https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html

[5] "Dahua New Critical Vulnerabilities 2021", https://ipvm.com/reports/dahua-21-critical?code=FCC

Dahua and Hikvision devices under American brands (e.g., Honeywell), this will unfortunately include devices in many Federal and military facilities.[6]

Dahua and Hikvision's responses has been to downplay these revelations, rather than proactively and widely communicate these risks (contrary to their marketing for case studies and other mundane announcements). Neither Dahua nor Hikvision has issued a press release, nor did they post an announcement on its home pages.

PRC Government Has Access To These Vulnerabilities

The PRC government has access to these vulnerabilities and may use them against the USA. Per PRC law, PRC companies, such as Dahua and Hikvision are directed to report these vulnerabilities to the PRC government within 2 days.[7] This means, at least for months, the PRC government has been able to use them against any of the millions of these PRC-made devices around the world, including the USA.

Moreover, these are only the latest issues in a long history of serious cybersecurity failures for both companies.

History of Critical Vulnerabilities

In October 2016, hackers exploited a Dahua vulnerability to turn their devices into bots, taking down various websites and ISPs (see: Mirai botnet attack). In September 2017, Dahua video recorders were mass hacked and vandalized around the world. In September 2019, 5 more Dahua vulnerabilities were found allowing attackers to execute malicious code on cameras. Numerous other examples can be found in our directory of surveillance cybersecurity vulnerabilities.[8]

Similarly, Hikvision's cybersecurity track record includes several past critical vulnerabilities.[9] Most famously, in March 2017, a backdoor was found allowing attackers to bypass authentication and gain admin access to Hikvision cameras. Hikvision initially obfuscated the seriousness of this hack until the Department of Homeland Security's ICS Cyber Emergency Response Team issued a notice, and rated its seriousness a 10.0 out of

---

[6] "Illegal Hidden Dahua and Hikvision Sales, Sellers and 'Manufacturers' Blame Each Other", https://ipvm.com/reports/feds-buy-banned-gsa

[7] 工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知 http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm

[8] "Directory of Video Surveillance Cybersecurity Vulnerabilities and Exploits", https://ipvm.com/reports/security-exploits?code=FCC

[9] ibid.

10.0.[10] Hikvision's code is relatively difficult to decompile, meaning many vulnerabilities may remain undiscovered; in February 2021, Lithuania's Ministry of Defense decompiled Hikvision's firmware, finding ~100 vulnerabilities.[11]

Hikvision and Dahua are security companies, yet their products have been riddled with serious security flaws that threaten networks on which they are installed. This contradiction raises the question of whether these vulnerabilities are only a result of negligence. In evaluating this, we urge the FCC to take into account Hikvision and Dahua's backgrounds as PRC controlled/affiliated entities.

PRC Government Control or Affiliation

Hikvision originated from the No. 52 Research Institute of the China Electronics Technology Group Corporation (CETC), a state enterprise created to supply electronics to the People's Liberation Army (PLA). CETC remains Hikvision's controlling shareholder to this day. The Director of the No. 52 Research Institute, Chen Zongnian, is a member of the National People's Congress; he is also Hikvision's Chairman.[12]

Hikvision has collaborated on missile research with the PLA. A study published on their site, conducted in collaboration with the PLA, examined how Hikvision could use their technology to improve the "lethality" of surface-to-air missiles, RPGs, artillery, and tanks. Hikvision has also been a Tier 1 supplier for the People's Liberation Army, the highest level of supplier.[13]

Dahua is privately-controlled by its founder & CEO, Fu Liquan, and his wife Chen Ailing; however, in March 2021, China-state owned China Mobile acquired ~10% stake in Dahua.[14] Fu Liquan, who is also Dahua's Communist Party Secretary, has told employees to "always follow the Party" and has described "political work" as "the top priority of private companies's Party building work."[15]

---

[10] "Hikvision Backdoor Confirmed", https://ipvm.com/reports/hik-backdoor
[11] Hikvision Cybersecurity Vulnerabilities Reported By Lithuania Government, https://ipvm.com/reports/hikvision-lithuania-vuln?code=FCC
[12] Hikvision: Created And Controlled By China PRC Government, https://ipvm.com/reports/hikvision-prc
[13] "Hikvision And China's Military", https://ipvm.com/reports/hikvision-prc-military
[14]State-Owned China Mobile Acquires 10% of Dahua https://ipvm.com/reports/china-mobile-dahua
[15] Dahua CEO Is Communist Party Secretary, Declares "Always Follow The Party", https://ipvm.com/reports/dahua-party?code=FCC

Non-PRC Alternatives

Unlike Huawei, Hytera, and ZTE that have minimal presence in the United States, Dahua and Hikvision have spent many years, spending tens of millions of dollars on sales and marketing to acquire dealers in the United States. This shows in a combined 100+ of those dealers petitioning the FCC not to proceed with its plan.[1617] Those comments overwhelmingly ignore both Dahua and Hikvision's history of critical cybersecurity vulnerabilities and Hikvision's PRC government creation and control.

Those dealer's main argument is lower cost products from Dahua and Hikvision but that lower cost is offset by the negative externalities and harm using these products cause for end-users and the public that suffer from these security issues.

Moreover, there are at least 40 manufacturers (not brands or relabellers but companies that develop their own video surveillance products) that would fill the gap including from the USA as well as allies including South Korea, Taiwan and the EU.[18]

Sincerely,

_____

John Honovich
President, IPVM
john@ipvm.com

_____

Conor Healy
Government Director, IPVM
chealy@ipvm.com

[16] 80+ Hikvision Partners Ask US FCC Not To Ban Hikvision
https://ipvm.com/reports/hikvision-fcc-not
[17] 20 Dahua Partners Ask FCC Not To Ban Dahua
https://ipvm.com/reports/dahua-fcc-not
[18] "40+ Alternatives to Dahua & Hikvision For Video Surveillance Camera Manufacturing, https://ipvm.com/reports/hikvision-dahua-alternatives-directory", https://ipvm.com/reports/hikvision-dahua-alternatives-directory?code=FCC